General Policy on Responsible Artificial Intelligence

COMPLAINCE AREA

PROSEGUR

VISIT…

LANZAROTE

Caliente.com

Contents

1. Owner 2
2. Scope........ 2
3. Purpose 2
4. Preparation and Approval 3
5. Implementation 3
5.1. Course........ 3
5.2. Principles of Responsible Artificial Intelligence 3
5.2.1. Respect for Human Autonomy........ 5
5.2.2. Principle of Prevention of Harm 5
5.2.3. Principle of Equity........ 5
5.2.4. Principle of Explainability 5
5.3. Assessment Requirements for Responsible AI 6
5.3.1. Human Action and Oversight........ 6
5.3.2. Technical Soundness and Safety 6
5.3.3. Privacy and Data Management........ 6
5.3.4. Transparency 7
5.3.5. Diversity, Non-Discrimination and Equity 7
5.3.6. Environmental and Social Well-Being 7
5.3.7. Accountability 7
5.4. Responsible Artificial Intelligence Methodology 8
5.5. Governance Model 8
5.5.1. Permanent Members of the Board........ 9
5.5.2. Non-Permanent Members 9
5.6. Roles and responsibilities........ 9
5.6.1. Ethics Officer........ 10
5.6.2. Group Data Protection Officer........ 11
5.6.3. Privacy Office 11
5.6.4. Legal Area........ 11
5.6.5. Information Security Area 12
5.6.6. Human Resources Area 12
5.6.7. Purchasing Area........ 12
5.6.8. Areas of Innovation and Information Technology........ 13
5.6.9. Business or Area Partner........ 13
5.7. Approval, revisions and changes to this Policy 13
5.8. Communication of this Policy........ 13
5.9. Confidentiality........ 14
5.10. Non-compliance 14
5.11. Review of the efficacy of the measures adopted........ 14
5.12. Glossary of terms 14
6. Related Documents 15

1. Owner

Corporate Director of Compliance.

2. Scope

This Responsible Artificial Intelligence Policy is applicable to all entities and employees that make up the PROSEGUR Group (hereinafter, "PROSEGUR") in all countries where PROSEGUR operates, and is binding on all personnel, internal or external, who may be involved in AI-related projects.

This Responsible AI Policy applies without prejudice to other policies, rules and procedures in force at PROSEGUR.

3. Purpose

PROSEGUR is firmly committed to respecting the rights and freedoms of the people involved in the course of its activity, as well as the importance of its solutions being respectful of ethical and moral values, and guaranteeing compliance with these values, as well as compliance with any applicable regulations.

In order to fulfil these purposes, PROSEGUR has drawn up this Responsible Artificial Intelligence Policy, which aims to lay the foundations of the methodology to be applied in all projects that incorporate AI, whether as a result of projects developed internally or as a consequence of the acquisition and implementation of external products or solutions, guaranteeing compliance with its three fundamental axes:

- **Lawfulness**: The AI must be **lawful**, so as to ensure compliance with all applicable laws and regulations;

- **Ethics**: The AI must also be **ethical**, i.e. it must ensure compliance with ethical principles and values; and finally,

- **Robustness**: The AI must be robust, both technically and socially, as AI systems, even if shaped by good intentions, can cause accidental harm.

4. Preparation and Approval

Drafted by:	Group Data Protection Officer				
Revised by:	Global Legal Area	Javier Aparicio Alfaro			
	Process Transformation Office				
	Corporate Compliance Director				
Approved by:	Data Protection Board			Date:	26/04/2022
Replacing:	Responsible Artificial Intelligence 3P General Standard	Edition:	01	Date:	17/01/2022

5. Implementation

5.1. Course

Artificial Intelligence (hereinafter "AI") is the ability of machines to use algorithms, learn from data and use what they learn to make decisions in the same way as a human being would.

In recent times, AI has become increasingly relevant in all areas of our lives, and we are finding more and more uses for it, both in the personal and professional spheres. However, while the use of AI-based technologies can bring significant benefits to users, the application of AI to the different areas of our lives requires the implementation of specific controls, policies and working methodologies to analyse and prevent the potential risks and/or harmful consequences that the use of AI technologies could generate for those affected, in terms of their rights and freedoms.

In order to guarantee the rights and freedoms of all persons who may be affected by the use of AI solutions and technologies, PROSEGUR has drawn up this Responsible Artificial Intelligence Policy.

PROSEGUR's Responsible Artificial Intelligence is defined as the set of ethical, moral, regulatory and security values applied to technological solutions that incorporate AI, with the aim of preserving the rights and freedoms of users who may be affected by the application of these technologies, making it possible to establish the limits, requirements and, in short, the rules of the game, both in internal Artificial Intelligence development projects and in the acquisition of solutions that incorporate the use of this technology.

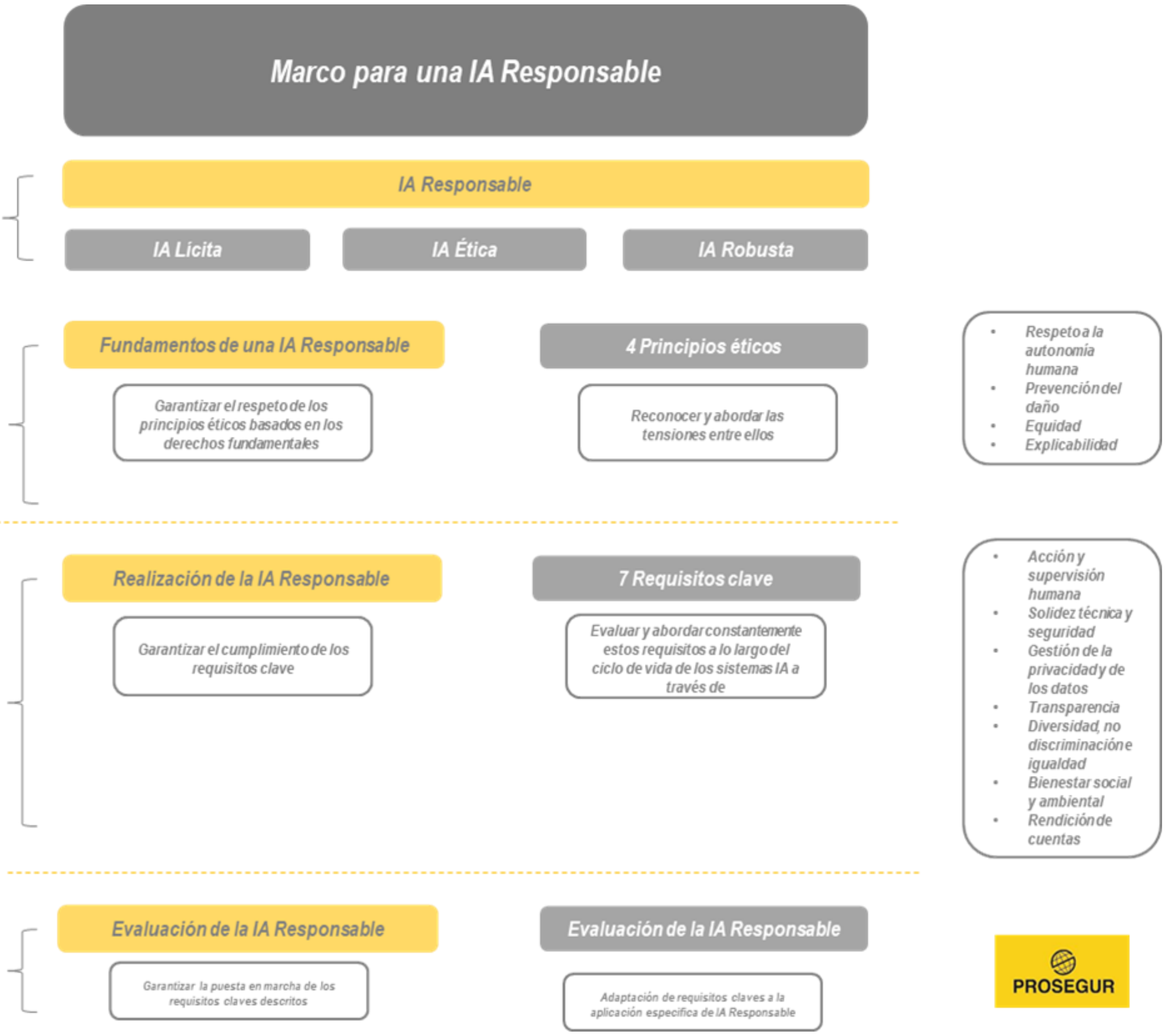
The application of this Responsible Artificial Intelligence policy will guarantee that the technological solutions developed in PROSEGUR, or acquired from third parties, are respectful of the organisation's ethical values and comply with regulatory requirements.

Within the practices included in this Responsible Artificial Intelligence policy, the importance of applying the "Ethics By Design" principle in all development projects that incorporate AI is of special relevance, which implies the need to apply ethics from the beginning in all AI technological development projects, so that the result of the solution is Responsible AI.

5.2. Principles of Responsible Artificial Intelligence

In drawing up this policy, PROSEGUR has taken as a reference the ethical principles set out in the *"Guide on Ethical Guidelines for Reliable AI" of the European Commission* , taking them as inspiring principles, whose observance must be present in all projects that incorporate AI technology, allowing for the improvement of individual and collective well-being.

In this regard, a graphical representation of the AI Framework for Responsible AI is shown below:


Marco para una IA Responsable
IA Responsable
IA Licita
IA Ética
IA Robusta
Fundamentos de una IA Responsable
Garantizar el respeto de los principios éticos basados en los derechos fundamentales
4 Principios éticos
Reconocer y abordar las tensiones entre ellos
Respeto a la autonomía humana
Prevención del daño
Equidad
Explicabilidad
Realización de la IA Responsable
Garantizar el cumplimiento de los requisitos clave
7 Requisitos clave
Evaluar y abordar constantemente estos requisitos a lo largo del ciclo de vida de los sistemas IA a través de
Acción y supervisión humana
Solidez técnica y seguridad
Gestión de la privacidad y de los datos
Transparencia
Diversidad, no discriminación e igualdad
Bienestar social y ambiental
Rendición de cuentas
Evaluación de la IA Responsable
Garantizar la puesta en marcha de los requisitos claves descritos
Evaluación de la IA Responsable
Adaptación de requisitos claves a la aplicación especifica de IA Responsable
PROSEGUR

In this sense, the four (4) principles that must be present in all projects for the development, acquisition or implementation of AI solutions by PROSEGUR are the following:

5.2.1. Respect for Human Autonomy

In the internal development and/or procurement of AI solutions, PROSEGUR shall ensure respect for the freedom and autonomy of human beings. AI systems will be designed in a way that augments, complements and enhances people's cognitive, social and cultural skills, which implies ensuring human supervision and control over the work processes of AI systems.

5.2.2. Principle of Prevention of Harm

PROSEGUR shall ensure that AI systems do not cause harm or otherwise damage human beings, protecting human dignity, as well as their physical and mental integrity.

PROSEGUR guarantees that all AI systems and environments are secure and robust from a technical point of view and will never be used for malicious purposes.

Likewise, PROSEGUR will pay special attention to the possible adverse effects that could be caused by an AI system, establishing specific measures for its mitigation, in order to prevent possible damage.

5.2.3. Principle of Equity

PROSEGUR ensures that the development, deployment and use of AI systems is equitable, committing to guaranteeing a fair and equal distribution of benefits and costs, and ensuring that individuals and groups are not unfairly biased, discriminated against or stigmatised.

PROSEGUR will endeavour to avoid unfair bias, and may establish specific measures to increase social equity through the use of AI systems.

Likewise, PROSEGUR's use of AI systems will respect the principle of fairness, understood as the ability to offer the possibility of opposing decisions taken by AI systems, as well as to convey its opposition to the people who operate them, and proportionality between means and ends, and will therefore carefully consider how to strike a balance between different interests and competing objectives.

5.2.4. Principle of Explainability

PROSEGUR is aware that explainability is crucial to gain user confidence in AI systems. To this end, all processes involving AI development are transparent, communicating clearly and concisely the capabilities and purpose of the AI system to the parties involved.

5.3. Assessment Requirements for Responsible AI

The following are the main requirements that an AI system must ensure in order to be a Responsible AI, which must be continuously assessed and addressed throughout the entire lifecycle of AI systems:

5.3.1. Human Action and Oversight

AI systems should support people's autonomy and decision-making, supporting human action and promoting fundamental rights, as well as enabling human oversight.

PROSEGUR will guarantee, as far as possible, a minimum of human intervention in the automated decision-making of AI systems, with the main purpose of preserving ethical, non-discriminatory decision-making that guarantees the rights and freedoms of the persons whose information is processed.

5.3.2. Technical Soundness and Safety

Technical soundness requires that AI systems are developed with a precautionary approach to risks, so that they always behave as expected and minimise unintended and unforeseen damage, and avoid causing unacceptable harm, while ensuring the physical and mental integrity of human beings.

In this regard, PROSEGUR will ensure that the AI systems are robust and comply with the appropriate security measures to guarantee the confidentiality, integrity and availability of the information stored and processed in them.

To this end, PROSEGUR will carry out rigorous security tests and evaluations to guarantee that the AI systems respond adequately to security incidents that could lead to the destruction, loss, accidental or illicit alteration, or unauthorised communication or access to the aforementioned information.

5.3.3. Privacy and Data Management

AI systems will observe the prevention of privacy harm, which implies appropriate data management, including data quality and integrity. Consequently, AI systems, their access protocols and their ability to process data will have to be developed without infringing on privacy.

PROSEGUR, as the controller or processor of personal data (as defined in the applicable regulations) that are processed in a processing operation that involves the use of AI systems, as well as the party responsible for AI-based systems, shall implement appropriate legal, organisational and technical security measures to guarantee the protection of the fundamental rights and freedoms of data subjects that may be affected, in strict compliance with the applicable data protection regulations. Likewise, PROSEGUR guarantees that only data that is strictly necessary for each of the intended purposes will be processed, limiting their retention to the necessary period of time, guaranteeing that they are not kept for longer than is necessary for the purposes of the processing.

5.3.4. **Transparency**

For an AI system to be transparent the following must have (i) **traceability**: the AI system's decisions are recorded in order to be able to identify the reasons for an erroneous decision by the system, which helps to prevent future errors, (ii) **explainability:** the decisions made by an AI system are understandable to humans and that they can track and (ii) **communicate with them**: that individuals are aware that they are interacting with an AI system and that the AI system should be identified as such and, where necessary, the user should be given the possibility to decide whether he/she prefers to interact with an AI system or with another person, in order to ensure compliance with fundamental rights.

5.3.5. **Diversity, Non-Discrimination and Equity**

For a Responsible AI system to be reliable, it needs to ensure inclusion, diversity, equal access, through unique design processes, as well as equal treatment throughout its life cycle.

In addition, in the internal development and/or acquisition of AI solutions, PROSEGUR will guarantee, in all cases, the equality and non-discrimination of persons who may be affected by their use, and in particular that exercised for reasons of race, colour, ethnic or social origins, sex, sexual orientation, age, genetic characteristics, language, religion or convictions, political opinions or any other type.

5.3.6. **Environmental and Social Well-Being**

PROSEGUR will promote sustainability and ecological responsibility through AI systems, and drive research into Artificial Intelligence solutions to address issues such as Sustainable Development.

5.3.7. **Accountability**

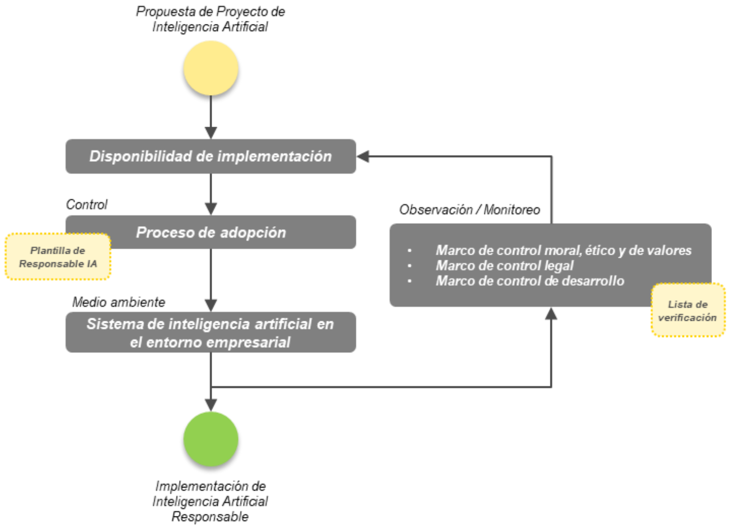
PROSEGUR has implemented mechanisms to ensure responsibility and accountability for AI systems and their results, both before and after implementation.

In this sense, PROSEGUR, as a promoter of the design and implementation of AI-based systems, will take responsibility for the actions and decisions taken by an AI system, especially as progress is made towards more autonomous systems capable of making automated decisions and, in particular, when such decisions have legal effects on the data subject.

In this regard, PROSEGUR has established a Responsible Artificial Intelligence Board, responsible for ensuring compliance with the ethical and moral principles and values described above, as well as their revision and updating in response to technological, social and regulatory advances that may affect the use of AI systems at any time.

5.4. Responsible Artificial Intelligence Methodology

PROSEGUR has developed and implemented a specific methodology for Responsible Artificial Intelligence, which allows it to achieve the purpose of respecting ethical and moral values, and to guarantee regulatory compliance, also promoting the use of this technology through internal development or the acquisition of AI solutions.


Propuesta de Proyecto de Inteligencia Artificial
Disponibilidad de implementación
Control
Plantilla de Responsable IA
Proceso de adopción
Medio ambiente
Sistema de inteligencia artificial en el entorno empresarial
Observación / Monitoreo
Marco de control moral, ético y de valores
Marco de control legal
Marco de control de desarrollo
Lista de verificación
Implementación de Inteligencia Artificial Responsable

Responsable del proyecto

- ✓ Modelo de negocio y finalidad de la solución.
- ✓ Crear requisitos.

Comité de Inteligencia Artificial

- ✓ Supervisar y garantizar el cumplimiento de la solución de IA en tres ejes: legal, ética y robustez técnica
- ✓ Definir los requisitos que se van a evaluar
- ✓ Evaluar objetivos, regulaciones, mejores prácticas y análisis de percepción.

Desarrollador de Inteligencia Artificial

- ✓ Diseñar, implementar y probar la solución.

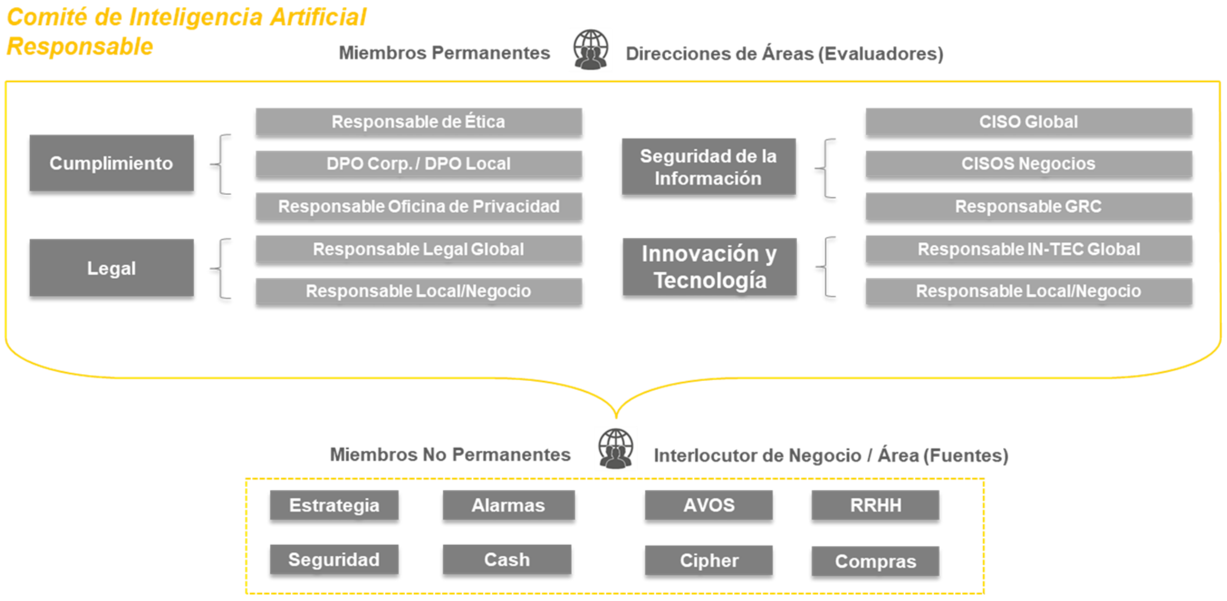
Operador de Inteligencia Artificial

- ✓ Implementar, ejecutar y supervisar la solución.

5.5. Governance Model

In order to comply with AI requirements and guarantee the defence of the rights and interests of stakeholders in the development of its activity, PROSEGUR has an AI governance model.

Below is a graphical representation of the Responsible AI Governance Model implemented in PROSEGUR, consisting of:


Comité de Inteligencia Artificial Responsable
Miembros Permanentes
Direcciones de Áreas (Evaluadores)
Cumplimiento
Responsable de Ética
DPO Corp. / DPO Local
Responsable Oficina de Privacidad
Legal
Responsable Legal Global
Responsable Local/Negocio
Seguridad de la Información
CISO Global
CISOS Negocios
Responsable GRC
Innovación y Tecnología
Responsable IN-TEC Global
Responsable Local/Negocio
Miembros No Permanentes
Interlocutor de Negocio / Área (Fuentes)
Estrategia
Alarmas
AVOS
RRHH
Seguridad
Cash
Cipher
Compras

PROSEGUR's Responsible AI Governance Model consists of a Corporate or Local Board, depending on whether the project covers several countries (Corporate) or a single country (Local), made up of the following bodies:

5.5.1. **Permanent Members of the Board**

- Compliance Management
- Data Protection Officer / Privacy Office
- Legal Area
- Innovation and Technology Area
- Information Security Area

5.5.2. **Non-Permanent Members**

- Strategy and Business stakeholders and/or the Areas promoting the development or acquisition of AI solutions

5.6. Roles and responsibilities

The Responsible Artificial Intelligence Board is a body of associates made up of the main heads of the areas involved and referred to in the previous section, whose main functions are:

- To ensure that AI projects and solutions that are procured or developed internally are accountable, impartial and comply with the four (4) principles enshrined in this Policy and set out in point 6 of this Policy.
- To supervise the development of all PROSEGUR's AI solutions, and monitor their entire life cycle, in order to ensure (i) strict compliance with applicable regulations and the requirements established for this purpose by PROSEGUR's corporate areas; (ii) the respect of ethical and moral values by these solutions, as well as (iii) the robustness of AI solutions from both a technical and social point of view.
- To keep a record of all AI solutions implemented in PROSEGUR.
- To advise the different areas on all legal and ethical issues affecting AI projects.
- To ensure that the requirements for reliable AI are met:
  - Human action and oversight,
  - Technical and security robustness,
  - Privacy and data management,
  - Transparency,

  - Diversity,
  - Discrimination and equity,
  - Environmental and social well-being,
  - Accountability.

- To communicate information to the areas involved, in a clear and proactive way, about the capabilities and limitations of AI systems, enabling realistic expectations to be set, as well as how requirements are being met. To be transparent about the fact that you are working with an AI system.

- To facilitate traceability and auditability of AI systems, especially in critical contexts or situations.

- To involve the relevant areas in the whole lifecycle of AI systems.

- To promote training and education, so that all areas involved are aware of Responsible AI and receive training on the subject.

The main roles and responsibilities of the members that make up the organisational structure of PROSEGUR's Responsible AI Governance Model are set out below.

5.6.1. **Ethics Officer**

- Oversees actions concerning compliance with ethical, legal and moral principles and respect for the dignity of persons affected by AI technologies., bearing in mind and addressing tensions that may arise between these principles.

- Pays special attention to situations affecting the most vulnerable groups, such as children, people with disabilities and others who have been historically disadvantaged or at risk of exclusion, as well as to situations characterised by asymmetries of power or information, such as those that may occur between employers and employees or between companies and consumers.

- In the event that the proposed AI solution is not approved by the Ethics Officer, no further action may be taken to implement or deploy the AI solution.

- Recognises and is aware that while AI solutions bring substantial benefits to individuals and society, AI systems may also entail certain risks that can have negative effects, some of which may be difficult to foresee, identify or measure.

- Takes appropriate measures to mitigate these risks where appropriate; such measures should be proportionate to the magnitude of the risk.

- Ensures that each AI project has a risk and contingency plan.

5.6.2. **Group Data Protection Officer**

- Promotes, coordinates and monitors the actions aimed at guaranteeing respect for and compliance with current regulations, principles and requirements in matters of Data Protection, when the solution involves personal data.

- In the event that the proposed AI solution is not approved by the Group DPO, no further action may be taken to implement or deploy the AI solution.

5.6.3. **Privacy Office**

- Advises and responds to doubts and queries regarding Data Protection, raised by the different Areas and Businesses of PROSEGUR on the occasion of the design or acquisition of solutions or projects involving the use of AI.

- Carries out the actions required to guarantee compliance with current data protection regulations and, specifically, to ensure compliance with the principle of Privacy by Design and by Default, in relation to the development of the different projects related to AI, provided that they affect or may affect personal data.

- Drafts and/or updates and implements policies, procedures, legal reports, privacy impact assessments, contractual documentation, clauses, as well as any other documents in the field of Data Protection whose drafting is necessary to provide legal certainty to AI projects, ensure compliance with the regulations, and ensure respect for the data protection principles established in the applicable data protection regulations.

- In the event that the proposed AI solution is not approved by the Privacy Office, no further action may be taken to implement or deploy the AI solution.

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.4. **Legal Area**

- Ensures compliance with applicable legal requirements with respect to projects or solutions that incorporate AI technologies, paying special attention to regulations on private security, intellectual property and those related to the use of software.

- Supports PROSEGUR's Innovation, Information Security, Procurement and Business areas in the analysis and review of legal requirements and contractual clauses that regulate the acquisition, development and use of AI solutions.

- Advises and gives legal support to the different Areas and Businesses involved in the Artificial Intelligence projects in PROSEGUR.

- In the event that the proposed AI solution does not have the approval of the Legal Area, no further action aimed at the implementation or deployment of the AI solution may be taken.

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.5. Information Security Area

- Ensures the correct definition and implementation of the technical and organisational security measures necessary to guarantee the security of the information processed in the development of AI projects, thus guaranteeing the confidentiality, availability and integrity of the data processed.

- Supervises and guarantees, in collaboration with the IT Area, the adequate implementation of the necessary technical measures to guarantee the IT security of the platforms, infrastructures, networks, databases and information systems involved in the AI projects.

- Establishes the information security requirements to be met by each PROSEGUR AI solution, and ensure strict compliance with them. To this end, the Information Security Area shall actively participate in the evaluation of PROSEGUR's potential suppliers, in order to guarantee that said suppliers and/or the solutions acquired from third parties comply with the established information security requirements.

- In the event that the proposed AI solution does not have the approval of the Information Security Area, no further action aimed at the implementation or deployment of the AI solution may be carried out.

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.6. Human Resources Area

- Ensures the protection of the rights and freedoms of employees and/or applicants who could potentially be affected by a PROSEGUR AI solution, especially with regard to their privacy, and ensure equality and non-discrimination.

- Reports to the Artificial Intelligence Board responsible for any initiatives carried out that may involve the use of AI systems, for the purpose of their evaluation, validation and follow-up

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.7. Purchasing Area

- Ensures the proper compliance with PROSEGUR's corporate supplier approval procedure, as well as coordinate, in collaboration with PROSEGUR's different support areas, the evaluation of suppliers contracted for the provision of services related to AI solutions, which requires an analysis of the supplier's degree of compliance with the requirements of the different support areas, namely legal requirements, data protection, intellectual property, information security, IT security, and those related to technical functionalities.

- Informs the Responsible Artificial Intelligence Board of the measures that the providers involved in AI solutions comply with the ethical and moral values and principles enshrined in this Policy, and, where appropriate, report to the Responsible Artificial Intelligence Corporate Board any incident of which they are aware in relation to the services provided by such providers.

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.8. Areas of Innovation and Information Technology

- Identifies the existence of PROSEGUR solutions or projects that may involve the use of AI and inform the Responsible Artificial Intelligence Board.

- Oversees that the AI is technically robust.

- Informs the Responsible AI Board of the potential launch of a new AI product or service, in such a way that the aforementioned solution can be adapted to the requirements established in this Policy, as well as comply with requirements demanded by the areas represented in the Responsible AI Board.

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

5.6.9. Business or Area Partner

- Reports to the AI Board on any initiatives that may involve the use of AI technologies.

- Designates an interlocutor from the corresponding business or area, so that he/she may (i) participate in the meetings of the Board held throughout the life cycle of the AI project, (ii) provide all the information or technical documentation that the Board may require, for the purposes of its analysis and study, and (iii) coordinate meetings or work sessions with the different stakeholders involved in the project and (iv) make him/herself entirely available to the AI Board in order to comply with the principles and requirements established in this Policy.

5.7. Approval, revisions and changes to this Policy

This Responsible Artificial Intelligence Policy is approved by PROSEGUR's Corporate Board for Responsible Artificial Intelligence, and is reviewed periodically in order to guarantee the correct adaptation of said Policy to the current regulations that may be applicable in the field of Artificial Intelligence, and to the current situation of the PROSEGUR Group.

To this end, PROSEGUR must ordinarily review it on an annual basis, and extraordinarily whenever there are variations in the strategic objectives or applicable legislation. Updates or amendments to this Policy will take place through the Corporate Responsible AI Board, where successive versions of this Policy are approved.

5.8. Communication of this Policy

This Policy shall be the object of appropriate dissemination, communication, training and awareness-raising actions for its timely understanding and compliance by the companies that make up the PROSEGUR Group.

The full text of this Policy is made available to all employees of the PROSEGUR Group, regardless of their activity and, in general, to all those persons to whom it is applicable in accordance with the provisions of this Policy, all of whom are obliged to strictly comply with its contents.

5.9. Confidentiality

This Policy is for the internal and exclusive use of PROSEGUR, and is therefore confidential. Any use other than that indicated is prohibited and must be expressly authorised.

Persons involved in the processing of personal data and information are obliged to maintain professional secrecy and confidentiality. This obligation shall continue even after the termination of their relationship with PROSEGUR.

5.10. Non-compliance

Failure to comply with any of the obligations contained in this Policy is considered a breach of the orders and instructions of PROSEGUR in its capacity as employer or entrepreneur, and PROSEGUR may reserve the right to take disciplinary, civil and/or criminal action as appropriate, on the grounds of such breach.

5.11. Review of the efficacy of the measures adopted

PROSEGUR undertakes to implement the methodology established in the area of Responsible Artificial Intelligence, as well as to monitor its effectiveness, with the main purpose of guaranteeing strict compliance with the objectives and principles enshrined in this Policy.

5.12. Glossary of terms

- **Responsible Artificial Intelligence** Board: Body of associates responsible for directing and supervising the actions of the PROSEGUR Group in the field of Artificial Intelligence.

- **Personal Data**. Any information relating to an identified or identifiable natural person; an identifiable natural person is any person whose identity can be established, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of that person's physical, physiological, ethical, moral, genetic, mental, economic, cultural or social identity.

- **Seed Data**: A set of source data from which a new Dataset is generated and used for training or use of Artificial Intelligence systems.

- **Summary Data**: A method for generating a new data set from a data set that retains the informational characteristics of the original data set, but does not allow the original data to be reconstituted from artificially created data, and therefore does not correspond to information about an identified or identifiable natural person.

- **Group Data Protection Officer**. Data Protection Officer at Global level, which in the scope of application of this Rule has the functions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. (GDPR).

- **Employee**. Any person, permanent or temporary, who provides labour or contractual services to PROSEGUR or who represents any of the Group companies.

- **Artificial Intelligence.** A combination of algorithms designed to create systems that have the same capabilities as those of a human being.

- **Artificial Intelligence Methodology**. Set of techniques and methods implemented to comply with the principles enshrined in this Responsible AI Policy.

- **Personnel**. All employees (internal staff) and collaborators (external staff) of the PROSEGUR Group at all levels, including but not limited to directors, managers, agency workers, volunteers, interns, agents, contractors and external consultants, among others.

- **Regulation on Artificial Intelligence**: Set of current regulations and mandatory requirements in the field of Artificial Intelligence.

- **Processing**. Any operation or group of operations performed on personal data or groups of personal data, whether or not using automated procedures, such as the collection, registration, organisation, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of access, checking or interconnection, limitation, deletion or destruction.

6. Related Documents

Code	Name
NG_GLO_CN_03	3P General Policy on Data Protection
DS_GLO_CN_04	3P Support Document for the Protocol on Dealing with the Rights of Data Subjects
DS_GLO_CN_03	3P Support Document for the Security Breach Management and Notification Protocol
DS_GLO_CN_02	3P Support Document for the Storage and Destruction of Data
DS_GLO_CN_01	3P Support Document for the Selection and Assessment of Providers
NE_GLO_CN_01	3P Specific Policy on Binding Corporate Rules (BCRs)
DS_GLO_CN_06	3P Support Document on Impact Assessment Protocol
DS_GLO_CN_05	3P Support Document for the Protocol on Managing BCR Claims and Requests
DS_GLO_CN_07	3P Supporting Document on the NCVs Advocacy Programme
DPIA	DPA_Providers_IA

EUS	System Usability Scale (EUS)_PROSEGUR
CEEPIA	AI Supplier Ethics Assessment Questionnaire
MFUAR	IAR_PROSEGUR Operating Manual
CESPD	Data Security and Data Protection Assessment Questionnaire
CEIAR	Responsible_AI Evaluation Questionnaire
PPIAR	Template_Projects_AI_Responsible_Template_Projects_AI_Responsible_Template_Projects_AI_Responsible
PVPLIA	Template_Verification_Legal_Principles_AI
PEDSIA	Template_Solution_Harm Assessment_AI
PRIIA	Template_Incident_Report_AI